# UNPACKING THE WHITE HOUSE NATIONAL CYBERSECURITY STRATEGY

## HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 23, 2023

**Serial No. 118–12**

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
*oversight.house.gov* or
*docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
51–668 PDF WASHINGTON : 2023

## COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
SHONTEL BROWN, Ohio
JIMMY GOMEZ, California
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
BECCA BALINT, Vermont
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Senior Policy Analyst
PETER WARREN, Senior Advisor
MALLORY COGAR, Deputy Director of Operations and Chief Clerk
CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director
CONTACT NUMBER: 202-225-5051

---

## SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida

# C O N T E N T S



## WITNESSES



*Opening statements and the prepared statement for the witness are available in the U.S. House of Representatives Repository at: docs.house.gov.*

## INDEX OF DOCUMENTS



*Documents are available at: docs.house.gov.*

# UNPACKING THE WHITE HOUSE NATIONAL CYBERSECURITY STRATEGY

**Thursday, March 23, 2023**

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
*Washington, D.C.*

The Subcomittee met, pursuant to notice, at 3:09 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcomittee] presiding.

Present: Representatives Mace, Timmons, Burchett, Edwards, Langworthy, Connolly, and Lynch.

Ms. MACE. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order. Welcome everyone, and good afternoon.

Without objection, the Chair may declare a recess at any time.

I recognize myself for the purpose of making an opening statement.

Good afternoon, and welcome to this hearing, the Subcommittee on Cyber, Information Technology, and Government Innovation. Today, we are going to discuss the White House National Cybersecurity Strategy, which was issued three weeks ago today. The strategy in this Administration's proposal for fighting a battle that, as a Nation, we must win. Key aspects of our everyday life now rely on the safe flow of data, computerized systems, and even AI. That includes the delivery of medical care, the conduct of law enforcement activity, the operation of utilities, and the smooth flow of ground and air transportation, and even critical infrastructure.

We must be able to trust the integrity of these systems, their ability to keep functioning, and to preserve and protect the data they use. When these systems fall victim to malicious hackers, the costs are enormous. And I don't have to remind our witness today, but in December 2020, with SolarWinds, we had 11 Federal agencies hacked by adversaries aligned with China and Russia. In my home state of South Carolina, a few summers ago, we saw the Colonial Pipeline hacked, and that is when we saw gas prices started to go up, and they really have never come back down since then. And so, this is an issue that is—affects everybody, whether in the public or the private sector.

Aside for the enormous costs, these breaches also erode trust in key institutions. So, for instance, the Federal Government com-

puter systems, holding confidential data of millions of Americans, has been compromised by malicious actors too many times. As I cited before, and most recently, D.C. Health Link, where we have been advised that over 50,000 people who use D.C. Health Link in the Federal Government work force, had been affected by that particular hack.

So, this is truly a national security issue. Many of the most sophisticated attacks come from abroad and target our critical infrastructure. In recent years, foreign hackers from China, Russia, and Iran have sought to disrupt our economy and society by infiltrating U.S. critical infrastructure systems, including airports, telecommunications networks, along with Federal and state government systems. I don't think I can open up my computer today and look at a news story and not hear about another cyberattack on one of our systems or one of our government, Federal, or state, or local agencies, that is everywhere. It is pervasive, and it is every day. We must have reliable safeguards against criminal and unauthorized use of data to ensure economic security, our homeland security, and our national security. This is going to require intelligent, coordinated action at the Federal level.

To help the executive branch rise to that challenge, two years ago, Congress created a new White House office to provide coherent direction and coordination to agency-level cybersecurity efforts across the Federal Government. That is a lot. You have a big shoes to fill, including by spearheading a National Cybersecurity Strategy. Prior administrations have released similar cybersecurity strategies, but this is really the first time it is to be issued since the Office of National Cyber Director was created into law.

We are pleased to have here today the acting head of the Office of National Cyber, Director, as our witness today. There are many burning questions that I have about implementation of the national cybersecurity strategy, so we all look forward to hearing from you this afternoon about the strategy document itself. I have it right here and discussing, you know, how and when the rubber meets the road, on how rhetoric can be translated into action either now or hopefully soon and in the future. But before I formally introduce our witness, I will yield to the Ranking Member Connolly to provide his opening remarks, and I yield back.

Mr. CONNOLLY. Thank you, Madam Chairwoman. Thank you for having the hearing, and welcome, Ms. Walden, this afternoon.

Cybersecurity is a defining political, economic, and national security challenge for our time. From malicious foreign actors' online destabilization and espionage campaigns to ransomware incidents that compromise government and private sector information technology networks, these attacks have cost the United States billions of dollars and countless critical strategic disadvantages. In Fiscal Year 2021 alone, U.S. Federal agencies, which depend on IT systems to carry out operations and protect the essential information, were the target of more than 32,500 cybersecurity incidents. In the last half of 2022, cyberattacks targeting governments jumped 95 percent worldwide and cost an average of $2.07 million per incident, a 7.25 percent increase from the previous year alone.

Data breaches also affect the private sector, including educational institutions and healthcare centers. In 2022, the FBI re-

ceived almost 801,000 phishing, personal data breach, and other complaints representing estimated losses of more than $10.2 billion dollars. According to a 2021 survey by research firm, AdvisorSmith, 42 percent of small-and medium-sized U.S. businesses had experienced a recent data breach—42 percent. The estimated average cost totals almost $9.5 million per breach, higher than any other country in the world, and 60 percent of organizations have raised prices on consumers to cover those costs. Experts now predict that the annual cost of cybercrime will climb to over $10 trillion in the next number of years.

Cyberattacks will eventually hit close to home for everybody. For Congress, it was most recently the hack of the D.C. Health Link, which operates the healthcare system used by most Members of Congress and our staff. Before that, it was the 2015 OPM data breach that exposed the private information of nearly 22 million individuals, including my own personal information. Cyber threats are not new, as information security has been on the Government Accountability Office's high-risk list since 1997.

For those who are concerned, you are right to be concerned, but we cannot just throw up our hands. We must act quickly and decisively to secure digital infrastructure, protect the integrity and confidentiality of data, and preserve public trust in government institutions. I am proud that Democrats in this Committee did just that and helped to lead the bipartisan fight to establish the Office of the National Cyber Director, the ONCD, in FY 2021. The ONCD is required to coordinate the whole of government effort to elevate American safety in the digital world, including through the development and implementation of the National Cybersecurity Strategy. I applaud this and look forward to hearing more from our witness today.

Drawing on bipartisan ideas, including those vested in the recommendations of the Cyberspace Solarium Commission, the Biden-Harris strategy, as presented, is a bold, comprehensive plan for government and industry to create a safer digital ecosystem for all Americans. Recognizing that cyber threats cut through all industries and ignore geographic borders, the plan will examine the regulatory landscape to harmonize cybersecurity standards across different sectors and around the globe. With so much at stake, it is critical that our regulatory landscape allow industry to focus on security outcomes, not duplicative or nonsensical compliance burdens. We also know that if hackers fail to break into one agency system, they will seek out vulnerable entry points elsewhere, and they do.

We must address the current patchwork of cyber regulations to ensure that cybersecurity protections flow seamlessly and efficiently across industries and government. The strategy realigns incentives to ensure that Federal Government's investments enhance the long-term strength of a cybersecurity posture. For example, it harnesses the Federal Government's purchasing power to shape market demand for safe and secure technologies. Through programs such as the Federal Risk and Authorization Management Program, FedRAMP, which this committee passed legislation forward that became law, we can bake into a product rather than an additional expensive feature.

Additionally, the strategy redistributes the responsibility so that those best positioned to protect the cybersecurity of our citizens, schools, hospitals, and small businesses are required to take reasonable steps to do so. For example, it embraces liability for software companies that fail to use best practices or take reasonable precautions to secure their own products. If we do not hold bad actors or actors more focused on sales than security accountable, we disadvantage responsible companies that take time to follow these best practices, and we increase systematic risk for our constituents.

As the Administration works to implement this strategy, Congress must provide the funding and clarify the authorities needed to ensure its success. As former chair of Government Operations Subcommittee and a current Member of this Subcomittee, I know it is essential that we invest in modernizing our legacy ID systems and recruit and maintain a Federal cyber work force for the future.

The Federal Government must improve its internal practices. It must reap the benefits of the latest cybersecurity technologies and increase cooperation with the private sector. I look forward to understanding how the ONCD will leverage this plan and collaborate with other congressionally empowered IT and cyber related leaders to promote the kind of accountability our critical Federal systems need. With that, I yield back.

Ms. MACE. Thank you, Mr. Connolly. I am pleased today to introduce our witness for the hearing. Ms. Kemba Walden is the acting director of the White House Office of National Cyber Director. Ms. Walden came to the ONCD from Microsoft, where she was the assistant general counsel in the company's Digital Crimes Unit. Prior to that experience, Ms. Walden spent a decade at the Department of Homeland Security, holding several counsel positions, including the Cyber and Infrastructure Security Agency. Welcome, Ms. Walden. We are pleased to have you this afternoon.

Pursuant to Committee Rule 9(g), the witness, if you will please stand and raise your right hand.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Ms. WALDEN. Aye.

Ms. MACE. Let the record show the witness answered in the affirmative.

We appreciate you being here today and look forward to your testimony and answering some of our questions. Let me remind the witness that we have read your written statement, and it will be here in full in the hearing record. Please limit your oral statement to five minutes today. As a reminder, press the button on the microphone in front of you so that it is on, and all Members up here can hear you. When you begin to speak, the light in front of you will turn green. After four minutes, the light will turn yellow. When the red light comes on, your five minutes has expired, and we would ask that you try to wrap it up at that juncture.

I recognize Ms. Walden to please begin her opening statement.

**STATEMENT OF KEMBA E. WALDEN, ACTING NATIONAL CYBER DIRECTOR, THE WHITE HOUSE**

Ms. WALDEN. Thank you. Thank you, Chairwoman Mace, Ranking Member Connolly, distinguished Members of the Subcomittee. Thank you for the privilege to appear before you today to discuss the Biden-Harris Administration's National Cybersecurity Strategy. I am eager to share with you how the President's strategy will make our digital ecosystem more secure and resilient. It builds on two years of the President's unprecedented attention on cyber issues as well as the resources and valuable leadership provided by Congress and this Committee. While my written testimony goes into more detail discussing each of the five pillars that make up the document, I would like to highlight the framing of the strategy and the two fundamental shifts in policy that are woven throughout it.

As you know well, the magnitude of the threat we face in cyberspace is real, but it is important to remember that we defend cyberspace not because it is some distant terrain where we battle our adversaries. We defend cyberspace because it is intertwined into nearly every aspect of our lives. We live in a world that is increasingly digitally dependent. Too often we are layering new technology onto old systems at the expense of security and resilience, and, unfortunately, today, an attack on one organization, industry, or state can rapidly spill over to other sectors and regions.

We all remember how the Colonial Pipeline ransomware attack, an incident affecting one company, resulted in a gas shortage impacting the entire East Coast. It is within these circumstances in mind that we crafted the President's National Cybersecurity Strategy—strategies or tools. At their most basic level, they match our goals where we are trying to go with the vision we need to get there.

In this strategy, our ultimate goal is a digital ecosystem that is more defensible, resilient, and aligned with our values. "Defensible" means we have tipped the advantage from attackers to defenders by designing systems where security is baked in, not bolted on. "Resilient" means that when defenses fail, which they sometimes will, the consequences are not catastrophic, and recovery is seamless and swift. Cyber incidents shouldn't have systemic real-world impacts, and in creating these conditions, we can and must seize the opportunity to instill America's values.

The strategy calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources. First, we need to rebalance the responsibility for managing cyber risk. Today, we tend to devolve responsibility for cyber risk downwards. We ask individuals, small businesses, and local governments to shoulder a significant burden for defending us all. We ask our parents and our kids to be vigilant against clicking suspicious links, and we expect school districts to go toe-to-toe with transnational criminal organizations, largely by themselves. This isn't just unfair, it is ineffective.

Instead, the biggest, most capable, and best positioned actors in our digital ecosystem can and should shoulder a greater share of the burden for managing cyber risk and keeping us all safe, and that includes the Federal Government. We must do a better job of

leading by example and defending our own systems, something I know is a key priority for this Subcommittee, but we expect similar leadership from industry, too. Our mantra is every American should be able to benefit from cyberspace, but every American should not have the same responsibility to keep it secure. Second, our economy and society must incentivize investments that make cyberspace more resilient and defensible over the long term. Doing that requires creating conditions so an entity is faced with trade-offs between easy, but temporary fixes and harder, but lasting solutions. They are motivated to choose the latter.

We need the free market and public programs, alike, rewarding security and resilience. That means building a robust cyber work force that draws from all parts of society and embracing security and resilience by design. A cybersecurity job should be in reach for anyone who wants one. These efforts also require thoughtful research and development, investments in cybersecurity to prepare for revolutionary changes in our technology landscape brought by artificial intelligence and quantum computing, and working with our allies and partners to promote the collaborative stewardship of our digital ecosystem.

A strategy is only as good as its implementation, and in implementing this strategy, the Federal Government will take a data-driven approach and will measure investments made, progress, and the outcomes and effectiveness of these efforts. Closely working with Congress, interagency partners, civil society, and the broader cybersecurity community will be key to getting this right and ensuring accountability. Work is already under way putting this strategy into action.

In conclusion, the President's strategy lays out how the United States will meet these challenges in cyberspace from a position of strength, leading in lockstep with our allies, and working with partners everywhere who share our vision for a brighter digital future. Thank you for the opportunity to testify, and I look forward to your questions.

Ms. MACE. Thank you, Ms. Walden, and we are asking about your mics, and I know you have been moving around. We apologize for that. I will now recognize myself for five minutes.

The National Cybersecurity Strategy, it really reads like a vision for the Federal Government, but real results, as you know, in your work in the private and public sector really depend on implementation of a vision or of a strategy. So, will you and your office be leading the implementation of the strategy, and if not, then who would be doing that? Where do we start with the strategy to do the implementation side of it?

Ms. WALDEN. Well, thank you, Chairwoman, for that question. One of the most exciting parts of the strategy for me is the last page where we articulate precisely that ONCD, in collaboration with OMB, are going to lead the development of this implementation plan. In fact, we have already started that work. ONCD was built to do that work. This is a plan that, as we articulate in the strategy, will be public, it will be developed, it is being developed, in full collaboration with all the departments and agencies who are going to be charged with certain action items, and with the private sector, and with civil society, and with Congress to make sure that

the strategy realizes the vision that we have laid out. This strategy is new and novel in my mind, because we have attempted to, where appropriate, place departments and agencies responsible for certain action items, and we will build that out in the implementation plan.

Ms. MACE. What do you think, the timeline? I mean, this is a big plan, a big strategy, but how long will it take to finally get there from point A to point B?

Ms. WALDEN. So, we have already started the work. We have created an implementation plan working group that we have convened other departments and agencies. We have started the actual implementation. So, for example, we have started crafting our work force awareness and education strategy. That is one of the implementation pieces. We have been implementing Executive Order 14028, which is that cybersecurity executive order putting actual action into place alongside of that or as part of that. We have been implementing our Zero Trust Architecture Strategy for the Federal enterprise to be more secure, layer by layer, piece-application by application. So, we have already started the work. We are moving full speed ahead. This will be an ever-evolving dynamic process because cybersecurity and cyberspace is ever evolving and dynamic, but we have already started the work.

Ms. MACE. And then, on the topic of work force, obviously we all agree here we want to build a robust cyber work force drawing from all parts of our society. I think everybody up here would agree with that. I am working on legislation to try to accelerate the hiring of Federal employees in the cybersecurity space, and I would look forward to working with you and your office on some of the ideas that we have from, you know, education to—in the way that we hire as well. But even under existing law, the executive branch has tools at its disposal it is not necessarily fully utilizing.

A report based on the findings of Solarium Commission cited specific actions the Administration could take now, should take now, and it calls for the office to help coordinate some of those actions. Your thoughts on that, and is that possible? Your thoughts on getting more employees. You know, as we have discussed before, we have an ageing work force. We have got four times as many people over the age of 60 in a lot of these jobs versus under the age of 30, and so at some point those individuals will retire. So, just sort of your thoughts. Will your office take the wheel and steer the effort to this more robust cyber work force?

Ms. WALDEN. So, yes, and in partnership with OPM. So, yes, we have similar concerns about access to good-paying cyber jobs for anybody that wants one, right? We need to be able to rethink the barriers that we might have imposed for those entry level jobs. We need to broaden the scope for how we bring in new employees, and perhaps we don't need people with four-year college degrees for——

Ms. MACE. Hundred percent, yes.

Ms. WALDEN. Maybe we look at community colleges. Maybe you just look at the digital skills. I have friends who are executives in the outside world there who are great at researching when they were younger. They have the right digital skills in order to be able to enter this work force.

In terms of the Federal cyber work force, I share a similar concern. And so, we are working with OPM to shore up and harmonize the differing Federal authorities across departments and agencies for hiring and retaining talent in this space. We are working with OPM to develop a legislative proposal, so, I would love the opportunity to work with you on those initiatives. But the idea is to make sure that we are not putting up or imposing barriers to recruitment and that we are also putting in incentives for retention.

Ms. MACE. Thank you, and I wish you the best of luck with the Director of OPM. We had her here two weeks ago. She was the worst witness our Committee has ever had in the two-plus years that I have been here. And so, I have much greater confidence in you and your leadership and hope like hell that you can pull that off with—because she really couldn't answer any of our questions about even workforce issues. So, I really hope and pray that you will be able to work with her, and she will be able to work with you, and us, too, to expedite getting Federal employees into our cyber workforce. So, thank you, and I yield back.

I will now recognize the Ranking Member Connolly for five minutes.

Mr. CONNOLLY. Thank you, Madam Chairwoman. Ms. Walden, if I could pick up a little bit on where Ms. Mace was, OK? We are looking at tens of thousands of positions in IT in the Federal Government and cyber as a subset of that, for sure. Given the age cohort of the Federal Government, right, we are looking at serious numbers of retirements over the next five years. So, how proactively—I mean you talked about removing barriers and working with OPM, but how do we proactively persuade, you know, the millennial generation 'you want to come work for the Federal Government, and we see a 30-year career in your future.' How do you do that? Do you go to college campuses, and how do we make Federal services attractive in the sphere when the private sector alternative is glaringly seductive in terms of compensation and benefits and everything else?

Ms. WALDEN. Well, thank you for that question, Representative Connolly. I personally do go to college campuses. I go to high schools. I even teach cybersecurity badge in my daughter's Girl Scout's troop. The pipeline is a serious part of our focus in the work force strategy. That is why we call it the work force and education strategy. We really need to not only focus on the core cyber and IT jobs and how we fill that, but the pipeline. So, in my experience, you cannot imagine yourself in a particular career unless you see yourself in that career. So, it is important to me, for example, to make sure that I am out there in front, motivating people to consider this.

So, a couple of thoughts about this. One, the thing that draws me in and out of the private sector and into the government is mission. Private sector cannot compete with the government on mission, and, quite frankly, the government cannot compete with the private sector on pay. We can do better, and that is one of the opportunities we are looking at in this new legislative proposal, being flexible and how we do pay. But what we really offer is mission as a sense of moral enlightenment, in many ways. So, yes, reaching out, reaching to rural areas of the United States, reaching into par-

ents to have parents understand the benefits of a career in cyber, and parents are and should be one of the primary influencers of their children. That is a constituency that I like to reach. But it is really the mission that is the secret sauce here.

Mr. CONNOLLY. Well, thank you. I will commend you. We have seen, for example, the excitement generated in high schools with robotics competition teams. The excitement is incredible, and I remember that some of our intelligence agencies actually sponsored cyber competitions. And so, we may want to think more about expanding that kind of program to get into high schools and get in people's heads this might be something you might want to pursue, including in Federal service.

Let me talk about the National Strategy. I mean, candidly, the National Strategy took a little while to get together. Now, granted, we were in a pandemic, and we have lots of other competing things, but cyber is not a new topic. The OPM breach occurred two administrations ago, affecting 22 million current and retired Federal employees, and so, it comes to us a little bit late. And I guess I am worried about implementation because we talk about a whole-of-government approach. Knowing the Federal Government, this Subcomittee and its predecessor have spent a lot of time looking at Federal agencies, the diversity of capability, the diversity of expertise, the diversity of proactive strategies to protect, you know, the jewels in a given agency is very variable. So, how are you going to have a whole-of-government approach that guarantees all Federal agencies, whether you are in intelligence or you are in education, are protected and that are proactively fending off and maybe even proactively attacking the bad guys?

Ms. WALDEN. What I can guarantee is that we are, as a whole of government, proactive in making sure that our systems are resilient. I feel the same urgency. I feel that we are moving like a bullet train in this space. There is a sense of urgency here. We want to get it right, though, so we have all of the departments and agencies working with us. We work by, with, and through them. We need mostly consensus to make sure that this moves forward in a deliberate, thoughtful, but expedient way, so I share that. That is why we were designed the way that we are as ONCD. So, we have been implementing, we have been working for the last two years on shoring up our cybersecurity resilience. I see my time is up.

Mr. CONNOLLY. Let me just say, because I know the Chairwoman shares my concern in this regard, I think you have got your work cut out for you.

Ms. WALDEN. I do.

Mr. CONNOLLY. And it is an across-the-board kind of thing. It is the IT we possess, the legacy systems that need to be retired. It is the encryption that hasn't happened or hasn't been updated. It is the personnel as the Chair pointed out, I mean, that the age gap between us and the private sector is phenomenal. And so, you know, I just think you have got limited resources, and your ability to try to have a cohesive strategy that affects everybody and protects everybody is going to be, well, I hope not a Sisyphean task. I am sorry, Madam Chairwoman. Thank you.

Ms. MACE. You are good. And it will be some of the Federal employees that won't want to go along with the national strategy that

is, as you said, it is preeminent. It is deeply important. I would now like to recognize Representative Timmons for five minutes.

Mr. TIMMONS. Thank you, Madam Chair. The National Cyber Strategy was expected to be released last fall. Was that delay a reflection of how difficult it is to get the various interested parties on the same page, or were there other challenges?

Ms. WALDEN. You know, it was a bureaucratic process intentionally so that we can make sure that everybody, every department and agency, saw themselves in the strategy and are ready to implement. So, that was just a necessary step that had to take place in order to make sure that it is successful.

Mr. TIMMONS. Sure. So, next question. U.S. businesses, no matter how hard they try to have the best cybersecurity possible, can still fall victim to nation-state attacks, and those attacks can often cost billions of dollars to publicly traded companies.

Mr. TIMMONS. Do you think that the Federal Government has a role in backstopping those businesses? Since, assuming they are doing everything possible to avoid an attack, it is just not possible to stand up to nation-state actors. What are your thoughts on that?

Ms. WALDEN. So, I will start by saying that the cyberspace is a global commons. It is a public good. So, the U.S. Government has a responsibility and a duty to make sure that it is safe, while the private sector pretty much owns and controls most of the infrastructure that underlines cyberspace. So, we have to work together.

So, my response to your specific question about small and medium businesses, one of the core tenants of the cybersecurity strategy is to make sure that those small and medium businesses don't bear the significant brunt of cybersecurity risk all on their own. So, all of the tools in the strategy are there to lift and shift that risk, while also making the infrastructure cyberspace more resilient. You talked about backstopping. That is indeed one of the tools that we are considering, so cyber insurance backstop. Think of flood insurance, for example, in order to make sure that cybersecurity, small and medium businesses, don't bear the full cost of a cybersecurity breach while we are also working on making sure that the systems are resilient.

Mr. TIMMONS. Sure. Thank you for that. So, let us talk about ICANN. The original intent was to promote the stability and security of the internet by creating a transparent multi-stakeholder governance model for the management of domain name system. So, in 2016, Department of Commerce, their role in ICANN expired. Do you have concerns over that, in the U.S.' leadership in maintaining a secure internet globally?

Ms. WALDEN. So, I think we need to consider how do we harmonize standards. Digital ecosystem is—doesn't have specific borders, so we need to make sure that we harmonize standards in general, but let me just even take it a step further back. Cyberspace is composed of three pieces. We have touched a lot on personnel, people, which is arguably the most important part of cyberspace, but it is also technology, the gizmos, the microphone that has an echo, all of that, right? But it is also governance, it is authorities and responsibilities. If no one is guarding the gate, then the bad guy can just walk through. It is that governance layer that you are getting at.

So, yes, the cybersecurity strategy, generally, is intended to articulate and find vulnerabilities in that governance layer, in the roles and responsibilities, figure out who is guarding the gates, figure out what the vulnerabilities are, and then close those vulnerabilities. So, that is a symptom of the challenge that we face.

Mr. TIMMONS. To that point, what tools does the Administration plan to use to bolster the security of the foundation itself?

Ms. WALDEN. So, there are a couple of tools as articulated in the strategy. I think it is Pillar 4 we talk about the technical opportunities in the foundations of the internet, right, like a faster migration to IPv6 from IPv4. That is one opportunity in terms of modernizing the backbone of the internet. But then there are also opportunities for filling those vulnerabilities, like I described, in the roles and responsibilities. The implementation plan is going to help us with that, at least in the departments and agencies. We are also looking at the idea of harmonizing standards, harmonizing regulations so that we know exactly what we are certifying to when we have like IoT device labeling, for example, how that works across borders, we collaborate with our allies. Pillar 5 talks about that. So, that is that roles and responsibilities piece that relates to the backbone of the internet.

Mr. TIMMONS. Sure. Thank you for being here today. Madam Chair, I yield back.

Mr. CONNOLLY. Madam Chairwoman, I just want to welcome to the Subcommittee the former Chairman of our full Committee and my predecessor in this seat in the 11th District, Virginia, the Honorable Thomas Davis. Welcome, Tom.

Ms. MACE. Thank you for joining us, sir. I would now like to recognize Representative—I turned my mic off for you—Burchett for five minutes.

Mr. BURCHETT. Thank you, Chairlady. You mentioned when we first started this that she doubted that I could spell AI, but I can assure you I can now. I have researched it. I Googled it. Ma'am, Chinese-owned media application, TikTok, has over 150 million active users in the U.S. Do you feel like this is a national security concern?

Ms. WALDEN. Yes.

Mr. BURCHETT. Another question. What countries do you think are the biggest threats to national cybersecurity?

Ms. WALDEN. Well, as articulated in the worldwide threats report that ODNI published, it is China, North Korea, Iran, and Russia.

Mr. BURCHETT. All right. 1,600 offshore oil and gas facilities faces significant risk of cyberattacks. What do you think the potential impact of a successful cyberattack on these facilities is, and what steps is your office taking to secure this infrastructure?

Ms. WALDEN. Please excuse me, I did not hear the very beginning of that question.

Mr. BURCHETT. I said six. OK. Yes, ma'am. I am sorry. I am from East Tennessee. It is the only place in the country where people do not speak with an accent.

Mr. CONNOLLY.

[Laugh]

Mr. BURCHETT. Thank you, Connolly. I appreciate it. 1,600 offshore oil and gas facilities faces significant risk of cyberattacks.

What is the potential impact of a successful cyberattack on these facilities, and what is your office doing to secure this valuable infrastructure?

Ms. WALDEN. Well, let me start with Pillar 1 of our National Cybersecurity Strategy, which is focused clearly on critical infrastructure security. There are several tools that we have identified in that pillar for making sure that we make our critical infrastructure more defensible, while also making investments in making sure that it is resilient regardless of the attacker or the type of attack. One of those opportunities is raising baseline cybersecurity requirements across all critical infrastructure sectors. There are many ways to do it, but as we do that, we need to make sure that no one, particular sector is overregulated so that we encourage investment in raising baseline cybersecurity requirements rather than investing in compliance. Now, with respect to the offshore oil rig, I would love to give you a reaction to that question, but I would need to research what the exposure is and——

Mr. BURCHETT. Please do. It has been recently reported, and I have been informed that that is a major issue, and I can assure you that if our enemies can turn that spigot off, they will.

Ms. WALDEN. Yes.

Mr. BURCHETT. And they will not do it in an environmentally sound manner either. If somebody could get with me from your office, that would be great.

Ms. WALDEN. Absolutely.

Mr. BURCHETT. From the cybersecurity perspective, ma'am, how can we better secure our global financial institutions from bad actors? I am always afraid they are going to turn the switch. In early days of eBay, they always said make sure you use PayPal. Everybody thought it was a racket, and it is a racket, but it is their racket, so it is just the deal. But then they would say, you know, you get wired money, and it was always some kind of lame deal, and people were always getting ripped off.

Ms. WALDEN. So, there are several opportunities. First, I would like to say about the financial services sector that they are quite mature in their cybersecurity practices. Of course, more work can always be done. As cybersecurity threat actors are always evolving and improving, so can our defenses, and so can our resilience, so it is an evolution. We work closely with the financial sector. We work closely with the Department of Treasury. So, for example, we have recently done exercises with the Department of Treasury for how do we make sure that our financial services sector becomes more resilient?

Mr. BURCHETT. Let me get to one more because I am running out of time.

Ms. WALDEN. OK.

Mr. BURCHETT. This is really important to me. Our senior citizens, they seem like they are on the radar for a lot of these dirtbags that prey upon them. And what steps can your office do to work with us to ensure that these folks are protected from these hostile foreign actors and groups?

Ms. WALDEN. My mom might hate me saying this on live C-SPAN, but I have got a mom who might be classified as a senior citizen, and it concerns me every time she does online banking.

Mr. BURCHETT. Mama had a Sunday school class and they called them "seasoned."

Ms. WALDEN. I like it.

Mr. BURCHETT. Well, she said, I did not like that, honey. It makes it sound like a bunch of cannibals, so my mama was a pretty cool lady. But go ahead, I am sorry.

Ms. WALDEN. No, but we need to make sure that all of the technology, all of the devices that we have, need security built in, right? We need to make that commercial where there is an easy button. That is what I envision when I am envisioning security built in for senior citizens. They should be able to turn on their computer, login is already enabled by default, multi-factor authentication is already enabled by default. All the different security options that you can take should be enabled by default. Security has to be built in.

Mr. BURCHETT. And I know we are out of time, but a recent former Director of the FBI got ripped off on one of these deals. And they went after them and got his money back, and I was glad they did that. But I was ticked off because I have had people that the FBI just gives me lip service, and if they could do it for one, they can do it for all of them, and dadgummit, they need to start doing it. So, thank you, ma'am.

Ms. MACE. Thank you, Mr. Burchett.

Mr. BURCHETT. I am sorry. I went out of time.

Ms. MACE. Are you yielding back?

Mr. BURCHETT. Do what?

Ms. MACE. Are you yielding back?

Mr. BURCHETT. Yes, ma'am, I yield——

Ms. MACE. Yes, you are. Yes, you are.

Mr. BURCHETT [continuing]. None of my time back.

Ms. MACE. All right. I would now like to recognize Representative Langworthy for five minutes.

Mr. LANGWORTHY. Thank you, Madam Chairwoman. Ms. Walden, I just want to thank you for being here today and providing this Subcommittee with the invaluable insight on the path forward in the cybersecurity sector.

So, I would like to start off by looking at cloud service providers. And the strategy correctly notes that cloud-based services enable better and more economical cybersecurity practices at scale, and their security is crucial for critical infrastructure in government systems. However, the strategy also is looking to close gaps in regulatory authorities for cloud services. Now, I am concerned that this categorical effort to sweep in an all cloud-based services is inconsistent with a risk-based approach. Can you explain the rationale for the blanket approach that you plan to pursue?

Ms. WALDEN. So, cloud service providers provide some cybersecurity risk protections, particularly for small and medium businesses, and even for large enterprises, so let us start there. The cloud service providers operate in a highly regulated environment as it is. They are a participant in all of the regulations that their customers bear. Wouldn't it be fantastic if we had harmonized system regulations so that those that are highly regulated and that cloud service providers provide the compliance for, equal—and we reward that investment and cause others to invest in cybersecurity best prac-

tices by looking at how they are regulated. But cloud services providers have publicly acknowledged—we have worked with them directly in developing the strategy, but they have publicly acknowledged the need for regulatory minimum cybersecurity requirements baselines to be brought up and for harmonization to take place.

So, cloud service providers, cloud environments are more secure than on-prem, but there is some work still to be done. And we are ready, willing, and able to work directly with cloud service providers, not necessarily to kowtow to their demands, but to make sure that we have effective harmonization across all sectors for these purposes of making cloud services more secure.

Mr. LANGWORTHY. You spoke in an interview recently saying that of cloud services, that if they were disrupted, they could create large and potentially catastrophic disruptions to our economy and to our government. Can you talk a little bit about this? You had mentioned how cyber criminals in malign foreign countries disrupt cloud services.

Ms. WALDEN. So, cyber criminals will typically spin up infrastructure using cloud services to do so. I was part of a team that would find that infrastructure and use all means appropriate to tear it down. I think that we can do that at scale. We need to be able to work with cloud service providers to remove infrastructure, or at least to harden infrastructure, so that cyber criminals cannot leverage it. Of course, there are other opportunities for making sure that we reduce or we increase the cost of cybercrime. We can arrest people. We can lean into our authorities more. But we also need to work with private sector, owners and operators of managed service providers, and cloud service providers to tear down infrastructure where infrastructure is being used by cybercriminals.

Mr. LANGWORTHY. OK. Now, the Stafford Act, generally speaking, is an all-encompassing document for disasters in the United States. A largescale cyberattack could plausibly be considered a disaster. However, cyber-related disasters are not mentioned in the Stafford Act. What would our strategy be in case of a large-scale attack?

Ms. WALDEN. This is the reason why we have designed the strategy the way that we have. We need to make sure that we have our ducks in a row so that we make it more defensible. But the focus really needs to be on what investments do we need to make in order to make sure that cyberattacks are not catastrophic and do not cause systemic failure or long-term failure, that we have shorter downtimes. We have a seamless response. So, that is the reason why we have the Cybersecurity Strategy. On your specific questions about the Stafford Act, I would be happy to come back to you with some thoughts about that, but that is the reason why we have the strategy the way it is.

Mr. LANGWORTHY. Thank you very much.

Mr. LANGWORTHY. And I yield back, Madam Chair.

Ms. MACE. Thank you. I would now like to recognize Representative Edwards for your five minutes.

Mr. EDWARDS. Thank you, Madam Chair. Ms. Walden, thanks for being with us. As I sit here and read your testimony and listen to your responses, I cannot think of a less enviable position than yours. We are certainly appreciative of you taking this on. I served

on a bank board for a number of years, and I knew the thing that kept us awake most at night was the chance of a cyber threat, and you have got a whole country to look out for. Can you see any, at this time, I do not want to talk about the plan so much, I want to talk about right now. Can you see any coordinated efforts from foreign governments right now to hack into systems in the United States, or are the threats out there from universities or just ne'er-do-wells or that sort of thing?

Ms. WALDEN. Thank you for that question. What I can say is that the Worldwide Threats Report that was published by ODNI is the preeminent description of cyber threats and nation-state actors. That is not classified. I would refer you to that, and I agree with everything that is in that report. If you are asking me about specifics, that might get into classified nature of a conversation, and I am not prepared to do that today.

Mr. EDWARDS. I respect that. Thanks. How do you coordinate with the private sector? We have all seen examples of how they, too, are under attack, and your responsibility is vast. How do you include the private sector?

Ms. WALDEN. You know, you can always just pick up the phone and call. So, there are opportunities, right? ONCD, my office, collaborated with the private sector in a robust way in a development of the strategy. We are not an operational office. We are, by design, a strategic policymaking office, but operationally, there are several different models. We need to meet the private sector where they are. We have recognized that we need proactive operational collaboration, and this is different than information sharing when I left government the last time. So, it is exciting for me to see how we are doing it now.

So, for example, CISA runs the Joint Cyber Defense Collaborative, known as the JCDC. It is a model where different private sector entities are able to come together, exchange ideas, exchange information with CISA, with each other. And there are other models like the National Security Agency's Cyber Collaboration Center, the CCC, which does cyber information sharing with their defense industrial base, maybe one-on-one, in a classified nature, however it is. But we need to meet the private sector where they are. We need to find opportunities to identify problems together, come up with solutions and operational plans for mitigating that problem together, and then executing and deploying that solution together.

Good example, one that makes me really excited and I think is a pivotal moment that really did inform the strategy, was that on the eve of, or the weeks leading up to the Russian invasion of Ukraine, we collectively, we the government, collectively figured out that we had intelligence that the private sector may not have. Understanding, particularly in the financial sector, that if we sanction Russia, that there might be some retaliatory effects on the financial sector here at home, that there is more that could be done with the intelligence that we had by those that actually operate and control the infrastructure in the financial services sector. We delivered that intelligence so that they can take action. We worked the intelligence. We worked the action together. And I would like to think that that is a success story. We did not see any retaliatory effect on the financial services sector.

Mr. EDWARDS. I am running out of time, but a question that has been burning on my mind for years, we have heard of this threat that maybe computers, PCs that we buy through foreign entities that may come from China, Korea, the chips may contain in their bias, some sort of code that is sniffing out activity here in the U.S. and just ready to be called whenever the foreign entity decides. Are you aware of that? Is that actually happening? Has it happened?

Ms. WALDEN. Well, I would like to point you to the strategy, and perhaps you might understand why the strategy talks about understanding the supply chain implications of chips manufacturing. That is partly what the CHIPS and Science Act is intended to mitigate, any opportunity like that, hypothetically, could happen like that. Wouldn't it be nice if we understood what was in our software, right, what code libraries were in our software and how they were assembled? Wouldn't it be nice if we could make sure that the final assemblers, for example, of software, were held liable for what is in it so that it is not buggy, or, and it does not have some nefarious code written into it.

That is one of the most intriguing parts of the National Cybersecurity Strategy, from my perspective, is how do we make sure that software is built with security in mind. How do we make sure that market focuses on securing the market rather than first to market? What are the incentives that we need to shift in order to make sure that that hypothetical situation does not happen?

Mr. EDWARDS. Thank you. Madam Chair, I yield.

Ms. MACE. Thank you. I am going to do one more quick round of questions. I may be the only one with questions, and then we are going to close it out, if that would be OK to the Ranking Member. I am going to recognize myself for five minutes and hopefully less than that.

One of my burning questions is on legacy systems. So, Y2K, I was learning COBOL, C++, we called it. COBOL was legacy back then in the late 1990's and early 2000's, and it is sort of shocking to me to see how many systems that we have that are still legacy today. So, for example, there is a 46-year-old Department of Education System handling 20 million student financial aid applications annually, running on COBOL. There is a 50-year-old HHS system supporting clinical and patient admin activities coded in C++. I mean, so the list goes on and on of all of these examples of these legacy systems. So you know, your thoughts on—the Government Accountability Office has pointed this out repeatedly we need these upgrades. We have needed it for decades. How does the strategy play into getting this done across the board?

Ms. WALDEN. You know, IT modernization is part of the story here. It has to happen. We cannot have 50-year-old systems.

Ms. MACE. It has to happen.

Ms. WALDEN. It has to happen.

Ms. MACE. I mean, there is—yes.

Ms. WALDEN. But it has to happen in a way that is smart and thoughtful, but it has to happen. There is some urgency behind it. We have already started working on that process.

Ms. MACE. What about the agencies and Federal employees that are dragging their feet on some of this? I mean, we have seen, like, at the VA right now, EHR, I mean, just taking over a decade to

do something that really should not take as long as it is. How do we get them to come along with this?

Ms. WALDEN. Well, I would love to take that particular question back about the VA and give you a detailed answer.

Ms. MACE. Yes.

Ms. WALDEN. But I share your urgency. I am 51.

Ms. MACE. And a lot of examples.

Ms. WALDEN. Yes.

Ms. MACE. I will not go into all of it. But the other quick thing I wanted to ask about, and you have talked about this, too. Our first hearing was on AI in this committee, and there are things that we cannot even imagine how AI will be used. I read a story the other day about ChatGPT getting through CAPTCHA, like, with a TaskRabbit employee, and told them that they were visually impaired, to break into that. We cannot even imagine how it might be used for good and then also for bad, which is one of my concerns. How are we going to use some of these tools to ensure that we defend ourselves against breaches that we cannot even be aware of right now? Where is AI? I know it is mentioned in the plan, but where do you see AI in the overall strategy?

Ms. WALDEN. So, it is mentioned in the strategy, but I think our first conversation was around AI at some point, and so, I have been giving this some thought. I think of AI and the cybersecurity pieces of it in three buckets, right? Data that fuels AI, the compute power for AI, and the algorithms. There are cybersecurity components of each piece of that, that we can use to not only shore it up so that it is not used for nefarious purposes, or at least we reduce the chances of it being used for nefarious purposes, but we can also use it for the benefit of security, right?

So, I am thinking in terms of data. I am thinking through data security measures, thinking through cryptography. How do we do data analytics without decrypting? Thinking about compute power and the work we are doing right now, as articulated in the strategy, on quantum is all about compute power. The work that we are doing on chip supply chain the gentleman here raised, it is all about compute power. And then the algorithms, how do we think about that? So, we are purposefully thinking through how to make sure that AI, the cybersecurity elements of AI, are used for good purposes, and that we are reducing the likelihood of——

Ms. MACE. We do not want China to eat our lunch or Russia, or Iran, or any of that.

Ms. WALDEN. Absolutely.

Ms. MACE. My last question is part of the strategy contemplates more regulation, but from your lips, God's lips to my ears, you said you did not want to overregulate. So, thank you for making that statement, much appreciated because I think that we could stifle innovation by overregulating. But in terms of regulation, that framework, who is going to coordinate the cybersecurity regulatory regime and then also de-conflict when that is necessary?

Ms. WALDEN. Well, we do have language, and not in this strategy, offering that ONCD in collaboration with OMB will lead a regulatory harmonization taskforce, for example, where we will think through precisely what are the gaps, what are the regulations, what are the authorities that exists now that we are underutilizing

for regulatory purposes of cybersecurity. How do we fill any gaps that might exist? But most importantly, you and I agree, that we need to harmonize so that we make sure that we incentivize investment in cybersecurity requirements and not compliance, which some sectors are doing right now.

And so, that is an all-of-department and—agency effort. We would love to have a task force that does that work. We are already working on that. We work on that through the CIRC, the Cyber Incident Response Council, and CIRCIA. We are working on that with independent agencies in terms of thinking through how do we harmonize the regulations that independent agencies are imposing, but there is more work to be done.

Ms. MACE. Thank you. And I would now like to recognize Representative Lynch for five minutes.

Mr. LYNCH. Thank you, Madam Chair, and I thank the Ranking Member for holding this hearing, and I want to welcome Ms. Walden for giving her testimony and helping the committee with this work.

Ms. Walden, the Administration's National Cybersecurity Strategy represents, I think, an important step in our response as a Nation in dealing with the cyber threat landscape. We know that autocratic and oppressive governments like Russia and China are not only operating full spectrum surveillance of their own citizens, but we also know that they are taking advantage of the freedoms that we have in our country by surveilling our personnel, our citizens as well. And they are leveraging espionage, influence campaigns, ransomware, critical infrastructure attacks, and emerging technologies to pursue all those goals.

Your strategy, as I read it, mentions "the dark vision for the future of the internet that the People's Republic of China and other autocratic governments," I presume, Russia, what "those regimes promote." Can you sort of flesh that out a little bit and talk about what does that look like, the dark vision that Russia and China present in terms of our future on the internet?

Ms. WALDEN. So, the way I think about the internet, is that it carries our values. It carries the values of those that design and build it. We have democratic values here. We need to lead and lean into that as we think about the future resilience of internet. We cannot allow autocratic societies like China, like Russia, to set our agenda to have internet, to have a cyberspace that we envision in the document that we presented here today. That is the idea. That is the big idea in this strategy is that we need to set what we think the future of cyberspace is. We need to invest in that future of cyberspace, and that is the resilience piece of it, rebalancing the risk piece of it. But we cannot let China, Russia, et cetera, et cetera, set our agenda. We are getting really great at defending against, but wouldn't it be great if we got in front of? That is a better opportunity from my perspective.

Mr. LYNCH. Absolutely.

Ms. WALDEN. That is what we mean.

Mr. LYNCH. OK. In some ways, and in frightening ways, this dark future that you identify in your National Cybersecurity Strategy, that dark future seems more immediate, to be honest with you. For example, *The Wall Street Journal* reported last week, and

I have an article here that I will ask for unanimous consent. It talks about China's use of state-sponsored hackers, teams of hackers, to employ novel hacking techniques.

Madam Chair, I ask unanimous consent to submit this *Wall Street Journal* article entitled, "Wave of Stealthy China Cyberattacks Hits U.S. and Private Networks, Google Says."

Ms. MACE. Without objection.

Mr. LYNCH. Thank you, Madam Chair. These techniques have allowed China to spy on governments and businesses for years without detection. These activities are so stealthy that, "The scope of Chinese intrusion into U.S. and Western targets is likely far broader than currently known." Ms. Walden, what solutions do we have in terms of—does the strategy include solutions to root out and combat these type of aggressive attacks by autocratic state actors, and how successful have we been thus far?

Ms. WALDEN. So, Pillar 2 of the strategy, in my mind, is quite aggressive and forward leaning. It really projects the concept that defense is the new offense in this space. But we need to lean further into the authorities that we do have to dismantle and disrupt while shoring up opportunities with the private sector to remove infrastructure that we know that these hackers are leveraging. So, there are opportunities for that, but really, what is going to happen here is we are going to have a cyberspace that is more resilient. There are going to always be some sort of holding our infrastructure at risk. We need to get in front of that. We cannot just keep playing whack-a-mole, essentially. That is the general idea. But I would direct your attention to Pillar 2 about our opportunities to disrupt and dismantle.

Mr. LYNCH. Thank you, Madam Chair. My time has expired, and I yield back. Thank you.

Ms. MACE. And I will recognize the Ranking Member Connolly for five minutes.

Mr. CONNOLLY. I thank the Chair, and I will not take five minutes. I do want to thank the Chair for holding this hearing, which is one of a series of hearings planned on cybersecurity, AI, IT management in general. And I just want to say thank you to Ms. Walden, but I also want to urge, and I know you share this view, Madam Chairwoman, we will have you back, and we are going to talk about implementation of the strategy because we are eager to see that happen.

And I do believe the task in front of you is herculean. A whole-of-government approach to this subject, noble, worthy, but very challenging, and we have been working a lot on those issues for a long time on this Subcommittee as predecessors. So, we certainly want to help, and we want to give you the opportunity to share successes and frustrations as we move forward.

I, also, Madam Chair, and then I will yield back. We talked earlier about hiring, and I just wanted to commend the three bills we are working on. One I have introduced, called the OPM Reform Bill to improve our hiring practices. The second I am working with Virginia Foxx, Congresswoman Foxx of North Carolina, called the Chance to Compete Act, which addresses what you were talking about earlier to Madam Chairwoman, to increase hiring of people with non-traditional credentials. And the third is the NextGen Fed

Employee Act, a bill I have introduced, which is to try to systematize and professionalize the use of internships in the Federal Government. We are so far behind the private sector in the use of internships to recruit the talent we need for the future, and I am working with Chairman Comer on that bill as well.

So anyway, we are working on trying to bolster how we hire, who we hire, and not only recruit but retain that work force of the future, and it is particularly acute and important in U.S. sphere. With that I yield back, and I thank the Chair.

Ms. MACE. Thank you, and in closing, and I agree with the Ranker, that this is a herculean effort, the tasks before you, but know that we are here to assist and help you. We will have you back. We are going to want to hear about implementation and how that is progressing along as well. The importance, as Representative Lynch said earlier, it seems like it is needed faster and faster. In particular, I am going back to AI, everything that I come back to, because it is advancing so quickly.

We just do not know what we do not know, and we do not know how it will impact us, the vulnerabilities that we have. And I have great concern, but not just the public sector, but the private sector, as well, on this issue, and so we want to offer as much support as we can. We will be putting out a portfolio of legislation to be helpful, and so in any way that any of us, you need us, you call us, and we will be there to assist here.

So, in closing, I want to thank Ms. Walden for her presence. Your testimony today was clearly knowledgeable. It was fantastic, and we really appreciate it. We are very interested to learn about how the Administration, as Congressman Connolly said, will implement this strategy, and we are going to want more details on that in our next conversation, and we will invite you back.

So, with that and without objection, all Members will have five legislative days within which to submit materials and to submit additional written questions for the witness, which will be forwarded to the witness for her response.

Ms. MACE. If there is no further business, and without objection, the Subcomittee stands adjourned.

[Whereupon, at 4:15 p.m., the Subcomittee was adjourned.]

○